



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/445,386	12/06/1999	Oleg Anatolovich Zolotorev	P-9902 MG	9876

7590 10/06/2003

Lackebach Siegel Marzullo  
Aronson & Greenspan  
Penthouse Suite  
One Chase Road  
Scarsdale, NY 10583

EXAMINER

GREENE, DANIEL L

ART UNIT	PAPER NUMBER
----------	--------------

3621

DATE MAILED: 10/06/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/445,386

Applicant(s)

ZOLOTOREV ET AL.

Examiner

Daniel L. Greene

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 06 December 1999.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-109 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-109 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

### *Claim Rejections - 35 USC § 103*

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-109 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen et al. U.S. Patent 6,072,870 [Nguyen], and in further view of Chaum U.S. Patent 4,987,593 [Chaum]

As per claims 1, 24, 48, 74, and 101:

Nguyen discloses the claimed invention except for the payment certificate signature is obtained by means of making a blind money signature of an operator. However, Nguyen does teach about the use of SET protocol with the use of keys and certificates/wallets for preventing the identity of the payer to the payee. Col. 87-88, lines 1-67.

Chaum teaches that it is known in the art to provide a payment certificate signature that is obtained by means of making a blind money signature of an operator. (Abstract).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to provide the payment gateway system utilizing SET protocol of Nguyen with the blind digital signature technique of Chuam, in order to further enhance the security of the transaction and the identity of the payer.

Nguyen discloses the claimed invention except for performing an operation of opening a payee's account. It would have been obvious to one having ordinary skill in the art at the time of the invention was made to performing an operation of opening a payee's account since it is known in the art that for a customer to conduct business with an entity, an account must be opened.

Nguyen discloses the claimed invention except for replenishing a payer device by an operation of primarily filling a payment certificate, in which a payment certificate base is created in the payer device and a payment certificate signature is obtained by means of making a blind money signature of an operator. It would have been obvious to one having ordinary skill in the art at the time of the invention was made to replenishing a payer device by an operation of primarily filling a payment certificate, in which a payment certificate base is created in the payer device and a payment certificate signature is obtained by means of making a blind money signature of an operator since it is known in the art that to create a payment certificate of value, monetary value must be assigned/attached to it. Col. 92, lines 14-63.

Nguyen discloses:

performing a payment operation in which the payment certificate signature and an identifier of the payment certificate base are included into payment data delivered to a payee device by means of which a payee order is formed including the payment certificate signature and the identifier of the payment certificate base; Col. 93, lines 5-40.

delivering the formed payee order to a payment server in which the payee's account is credited on the basis of the payee order in the case of absence of an information that the payment certificate was utilized, according to the validity of the delivered payment certificate signature; Col. 21, lines 19-67.

forming the operator's response to the payee order, by means of which response the payment operation is judged, *characterized* in that the method is further comprising steps of including an identifier of a public key into the payment certificate base, said public key corresponding to an arbitrary secret key of a payer, wherein the public key is accepted as a public key of the payment **certificate and the** secret key of the payer is accepted as a secret key of the payment certificate; Col. 23, lines 17-61.

including a payer order signed with the secret key of the payment certificate into the payment data, and including information on the payee and the identifier of the payment certificate base into the payer order; Col. 20, lines 18-67.

the step of crediting the payee's account is carried out according to the validity of the signature on the payer order. Col. 22, lines 10-25.

Per claims 2, 28, 51, and 77:

Nguyen discloses the claimed invention except for the step of performing the payment operation the signed payer order is entered into the operator's information storage. It would have been obvious to one having ordinary skill in the art at the time of the invention was made to the step of performing the payment operation the signed payer order is entered into the operator's information storage since it is known in the art that during a commercial transaction involving computers, the transaction is entered into storage/memory on the respective participants systems.

As per claims 3, 25, 52, 78, and 104:

Nguyen discloses the claimed invention except for the payment certificate signature is obtained by means of making a blind money signature of an operator. However, Nguyen does teach about the use of SET protocol with the use of keys and certificates/wallets for preventing the identity of the payer to the payee. Col. 87-88, lines 1-67.

Chaum teaches that it is known in the art to provide a payment certificate signature that is obtained by means of making a blind money signature of an operator. (Abstract).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to provide the payment gateway system utilizing SET protocol of Nguyen with the blind digital signature technique of Chuam, in order to further enhance the security of the transaction and the identity of the payer.

Nguyen discloses the claimed invention except for the term “unblinding” . It would have been obvious to one having ordinary skill in the art at the time of the invention was made that the term unblinding refers to decrypting the data for viewing since it is known in the art that when you decrypt data, you expose or unblind the data for processing.

Nguyen further discloses:

*characterized* in that in the step of replenishing the payer device a money demand is formed including data for making a blind money signature, and is delivered to the payment server in which a replenishment source and replenishment amount are determined according to the money demand; data to be unblinded are created in the step of making the blind money signature by processing data for making the blind money signature, that are comprised in the demand, with a secret money key corresponding to the replenishment amount, whereupon the payment certificate signature is made in the payer device by unblinding. Col. 87-88, lines 1-67.

As per claims 4, 26, 27, 53, 79, and 80:

Nguyen further discloses:

The method according to claim 3, *characterized* in that in the step of replenishing the payer device by the operation of primarily filling the payment certificate a blinded identifier of the created payment certificate base is included as the data for making the blind money signature into the money demand being formed. Col. 20, lines 18-50.

As per claims 5, 54, 81, and 99:

Nguyen further discloses:

*characterized* in that in the step of performing the payment operation a payee receipt is included into the operator's response to the payee order, which receipt being signed with the arbitrary secret key of the operator, and the performing of the payment for the payee is judged according to the validity of the signature on the payee receipt.

Fig. 12.

As per claims 6, 30, 55, and 82:

Nguyen further discloses:

*characterized* in that in the step of performing the payment operation data are formed in the payee device with the use of the operator's response to the payee order and delivered to the payer device, according to which data the performing of the payment for the payer is judged. Fig. 14.

As per claims 7, 31, 56, and 83:

Nguyen further discloses:

*characterized* in that in the step of performing the payment operation a payer receipt is included into the operator's response to the payee order and into the data delivered to the payer device, which receipt being signed with the arbitrary secret key of the operator, and the performing of the payment for the payer is judged according to the validity of the signature on the payer receipt. Fig. 15A.



As per claims 8, 32, 57, 84:

Nguyen further discloses:

*characterized* in that the payer receipt is encrypted by an arbitrary encryption key of the payer prior to including said receipt into the operator's response to the payee order. Fig. 10.

As per claims 9, 33, 58, and 85:

Nguyen further discloses:

*characterized* in that in performing operations with the payment certificate the public key of the payment certificate converted by an arbitrary one-way function is used as the identifier of the payment certificate base. Fig. 10.

Nguyen discloses the claimed invention except for the term arbitrary. It would have been obvious to one having ordinary skill in the art at the time of the invention was made to replace the term arbitrary with the term random since it is known in the art that arbitrary and random are one in the same for function.

As per claims 10, 34, 59, and 86:

Nguyen discloses the claimed invention except for *characterized* in that in performing operations with the payment certificate the public key of the payment certificate is used as the identifier of the public key of the payment certificate. It would have been obvious to one having ordinary skill in the art at the time of the invention was

Art Unit: 3621

made to *characterized* in that in performing operations with the payment certificate the public key of the payment certificate is used as the identifier of the public key of the payment certificate since it is known in the art that in performing operations with the payment certificate the public key of the payment certificate is used as the identifier of the public key of the payment certificate.

As per claims 11, 35, 60, and 87:

Nguyen further discloses:

*characterized* in that in the step of replenishing the payer device the validity of the made payment certificate signature is verified. Col. 22-23, lines 1-67.

As per claims 12, 36, 61, and 88:

Nguyen further discloses:

*characterized* in that in the step of opening the account an arbitrary secret key is accepted as the secret key of the account, and the public key corresponding to the secret key of the account is delivered to the payment server as a public key of the account being opened. Col. 16-17, lines 1-67.

As per claims 13, 37, 62, and 89:

Nguyen further discloses:

*characterized* in that conditions of payment are included into the payer order. Fig. 6.

As per claims 14, 38, 63, and 90:

Nguyen further discloses:

*characterized in* that payee obligation data are included into the conditions of payment comprised in the payer order. Fig. 26.

As per claims 15, 39, 64, and 91:

Nguyen further discloses:

*characterized in* that prior to performing the payment operation, the payee obligation data are signed with an arbitrary secret key of the payee, and the payer verifies the payee's signature on the payee obligation data prior to performing the payment operation. Col. 18, lines 1-67.

As per claims 16, 40, 65, and 92:

Nguyen further discloses:

*characterized in* that in the payer device in the step of forming the payment data, the payee obligation data are processed by an arbitrary one-way function, and data obtained in this processing are included into the payer order as the conditions of payment. Fig. 4.

As per claims 17, 41, 66, and 93:

Nguyen further discloses:

*characterized* in that the payer order is encrypted by an arbitrary public encryption key of the operator prior to including them into the payment data. Col.16, lines 39-67.

As per claims 18, 42, 67, and 94:

Nguyen further discloses:

*characterized* in that in the step of replenishing the payer device a payer's account is used as a replenishment source. Col. 87-88, lines 1-67.

As per claims 19, 43, 68, and 95:

Nguyen further discloses:

*characterized* in that in the step of replenishing the payer device a bankcard is used as a replenishment source. Col. 24, lines 40-50.

As per claims 20, 44, 69, and 96:

Nguyen discloses the claimed invention except for in the step of performing the payment operation the payee appears as the payer. It would have been obvious to one having ordinary skill in the art at the time of the invention was made to in the step of performing the payment operation the payee appears as the payer since it is known in the art that that a merchant is a payee when distributing material and a payer when purchasing merchandise.

As per claims 21, 45, 70, 97:

Nguyen further discloses:

*characterized* in that in the step of performing the payment operation a part of a payment certificate value is returned to the payer device. Col. 38-39, lines 1-67.

As per claims 22, 46, 72, and 98:

Nguyen further discloses:

*characterized* in that the step of replenishing the payer device is performed from funds of an intermediate payer. Col. 89, lines 50-67.

As per claims 23, 47, 73, and 99-100:

Nguyen further discloses:

*characterized* in that in the step of replenishing the payer device, data blinded in the payer device in the step of making the blind money signature of the operator are subjected to an additional blinding in the payer device of the intermediate payer. Col. 16-17, lines 1-67.

As per claims 49, and 75:

Nguyen discloses the claimed invention except for *characterized* in that the payment account associated with the payment certificate base is opened in the step of performing the payment operation. It would have been obvious to one having ordinary

Art Unit: 3621

skill in the art at the time of the invention was made to *characterized* in that the payment account associated with the payment certificate base is opened in the step of performing the payment operation since it is known in the art that to perform a payment operation you must open the payment account the action is associated with.

payment certificate base is opened in the step of performing the payment operation.

As per claims 50, and 76:

Nguyen discloses the claimed invention except for the crediting operation is carried out in the step of performing the payment operation.

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to the crediting operation is carried out in the step of performing the payment operation since it is known in the art that when a payment is made, credit is recorded in an accounts payable account.

As per claim 71:

Nguyen further discloses:

*characterized* in that in the step of replenishing the payer device, a payment account associated with the base of one of payment certificates is used as a replenishment source. Col. 42, lines 1-10.

As per claim 102-103:

Nguyen further discloses:

*characterized* in that the payee device comprises a means for opening a public key account, and said means for serving the database of accounts has a means for opening a public key account. Col. 15-16, lines 1-67.

As per claim 105:

Nguyen discloses the claimed invention except for serving the database of payment accounts has a means for opening a payment account and a means for crediting a payment account.

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to serving the database of payment accounts has a means for opening a payment account and a means for crediting a payment account since it is known in the art that serving the database of payment accounts has a means for opening a payment account and a means for crediting a payment account.

As per claim 106:

Nguyen further discloses:

*characterized* in that the payee device has a means for verifying the signed payee receipt. Col. 14, lines 1-67.

As per claim 107:

Nguyen further discloses:

*characterized* in that said means for forming the payer order signed with the secret key of the payment certificate has a means for forming a demand for crediting the payment account. Col. 21-22, lines 1-67.

As per claim 108:

Nguyen further discloses:

*characterized* in that said means for forming the demand for crediting the payment account has a means for decreasing the level of the payment certificate signature. Col. 90-91, lines 1-67.

As per claim 109:

Nguyen further discloses:

*characterized* in that the payer device, payee device and payment server are further provided with a means for encryption of outgoing messages and a means for decryption of incoming messages. Col. 14, lines 1-67.

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant.

Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures



Art Unit: 3621

may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Greene whose telephone number is 703-306-5539. The examiner can normally be reached on M-Thur. 8am-6pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James P. Trammell can be reached on 703-305-9768. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-1113.

9/25/03

DLG

  
JAMES P. TRAMMELL  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 3600